# 22. Active Directory - Hardening

## 🧠 1. Understanding Active Directory Architecture & Security Threats

### 🏛️ Core Components

- **Domain Controllers (DCs)** – Servers that handle AD authentication/authorization.
- **Domains** – Logical groupings of users/computers under a single security boundary.
- **OUs (Organizational Units)** – Containers for organizing users, groups, and policies.
- **Trust Relationships** – Allow access across domains/forests.

### 🚨 Common AD Security Threats

- **Pass-the-Hash (PtH)**
- **Kerberoasting**
- **Golden Ticket Attacks**
- **Credential Dumping (Mimikatz)**
- **Privilege Escalation via GPO Misconfigurations**
- **Weak/Shared Local Administrator Passwords**

---

## 🔐 2. Securing Domain Controllers (DCs)

### 📌 Best Practices:

- **Physical Security** – Restrict physical access to DCs.
- **Network Isolation** – Place DCs on isolated VLANs with strict firewall rules.
- **Patch Management** – Regular OS and AD patching.
- **Limit Admin Access** – Use tiered administrative models (Tier 0 for DCs).
- **Disable Unnecessary Services/Ports** – Reduce attack surface.

---

## ⚙️ 3. Group Policy Objects (GPOs) for Security Enforcement

### 🔑 Key Security Policies:

- **Account Lockout Policies**
- **Password Complexity & Expiration**
- **Logon Restrictions (Smart card required, hours)**
- **Restricted Groups / Admin Rights Management**
- **Software Restriction or AppLocker Policies**

📚 **Pro Tip**: Regularly audit GPOs for changes using advanced auditing and tools like `gpresult`, `RSoP`, or GPMC.

---

## 🌐 4. Network Security for AD

### 🔐 Critical Network Protections:

- **Restrict LDAP/LDAPS Traffic**
- **Implement SMB Signing**
- **Use IPSec to Encrypt Traffic**
- **Disable NTLM where possible**
- **Limit RDP and admin tools to jump servers**

🛡️ **Defensive Tools**:

- Network segmentation (internal firewalls)
- Detection systems (IDS/IPS)
- Harden DNS and DHCP servers

---

## 📋 5. Advanced Auditing + SIEM Integration

### 🔍 Configure Advanced Audit Policy:

Enable auditing for:

- **Logon Events (4624, 4625)**
- **Privilege Use (4672)**
- **Object Access (4663, 4662)**
- **Account Management (4720–4732)**

📤 **Send logs to a SIEM** like:

- **Splunk**, **ELK**, **Graylog**, **Microsoft Sentinel**

Benefits:

- Real-time alerts
- Historical search and correlation
- Threat hunting and forensics

---

## 🛠️ 6. Mitigating AD Attacks

| Threat | Mitigation |
|---|---|
| **Kerberoasting** | Use long/complex SPN account passwords, monitor TGS requests |
| **Golden Ticket** | Secure and monitor `krbtgt` account, reset regularly |
| **Pass-the-Hash** | Disable NTLM, use Credential Guard |
| **Credential Dumping** | Enable LSASS protection, restrict debug rights |
| **Lateral Movement** | Use Just-In-Time (JIT) admin access, tiered accounts |

---

## 🔑 7. Introduction to LAPS (Local Administrator Password Solution)

LAPS is a Microsoft solution to:

- Randomize local admin passwords on domain-joined computers.
- Store them securely in **AD attributes**.
- Allow authorized users to retrieve them.

### 🧩 Why Use LAPS?

- **Prevents password reuse across machines**.
- **Mitigates lateral movement** (no shared local admin passwords).
- **Ensures compliance** with password complexity and rotation policies.

---

## 🧰 8. Configuring LAPS Step-by-Step

### ✅ Prerequisites:

- AD schema extension (`ms-Mcs-AdmPwd`, `ms-Mcs-AdmPwdExpirationTime`)
- LAPS installed on client and management machines.

### 🧱 AD Configuration:

```
Import-Module AdmPwd.PS
Update-AdmPwdADSchema
Set-AdmPwdComputerSelfPermission -OrgUnit "OU=Workstations"
Set-AdmPwdReadPasswordPermission -OrgUnit "OU=Workstations" -AllowedPrincipals "Helpdesk"
Set-AdmPwdResetPasswordPermission -OrgUnit "OU=Workstations" -AllowedPrincipals "Helpdesk"
```

### 🔧 GPO Configuration:

Configure via Group Policy:

- **Enable local admin password management**
- **Set password complexity/length**
- **Set password age (expiration)**
- **Configure access control for password retrieval**

📍 Location:
`Computer Configuration > Administrative Templates > LAPS`

---

## 🔍 9. Retrieving LAPS Passwords

### 🔓 Methods:

- **PowerShell**:

  ```
  Get-AdmPwdPassword -ComputerName "PC-001"
  ```

- **LAPS UI Tool**: Graphical interface for helpdesk.
- **Attribute Viewer in ADUC**: Check `ms-Mcs-AdmPwd`

---

## 🧩 10. LAPS + Security Best Practices

- **Audit who retrieves passwords** using event ID `4662`.
- **Rotate passwords** frequently (every 1–7 days).
- **Do not store local admin passwords in Group Policy Preferences!**
- **Only grant retrieval rights to trusted roles (Helpdesk, Security team)**.

---

## ✅ Summary

| Area | Skill/Knowledge |
|---|---|
| AD Security | Understand structure, threats, and attack techniques |
| Domain Controller Hardening | Patch, restrict access, isolate |
| GPO Usage | Enforce security baseline |
| Network Protections | Secure protocols and segmentation |
| SIEM Integration | Monitor AD activity in real time |
| Attack Mitigation | LAPS, auditing, credential protection |
| LAPS Management | Install, configure, retrieve, audit |

---